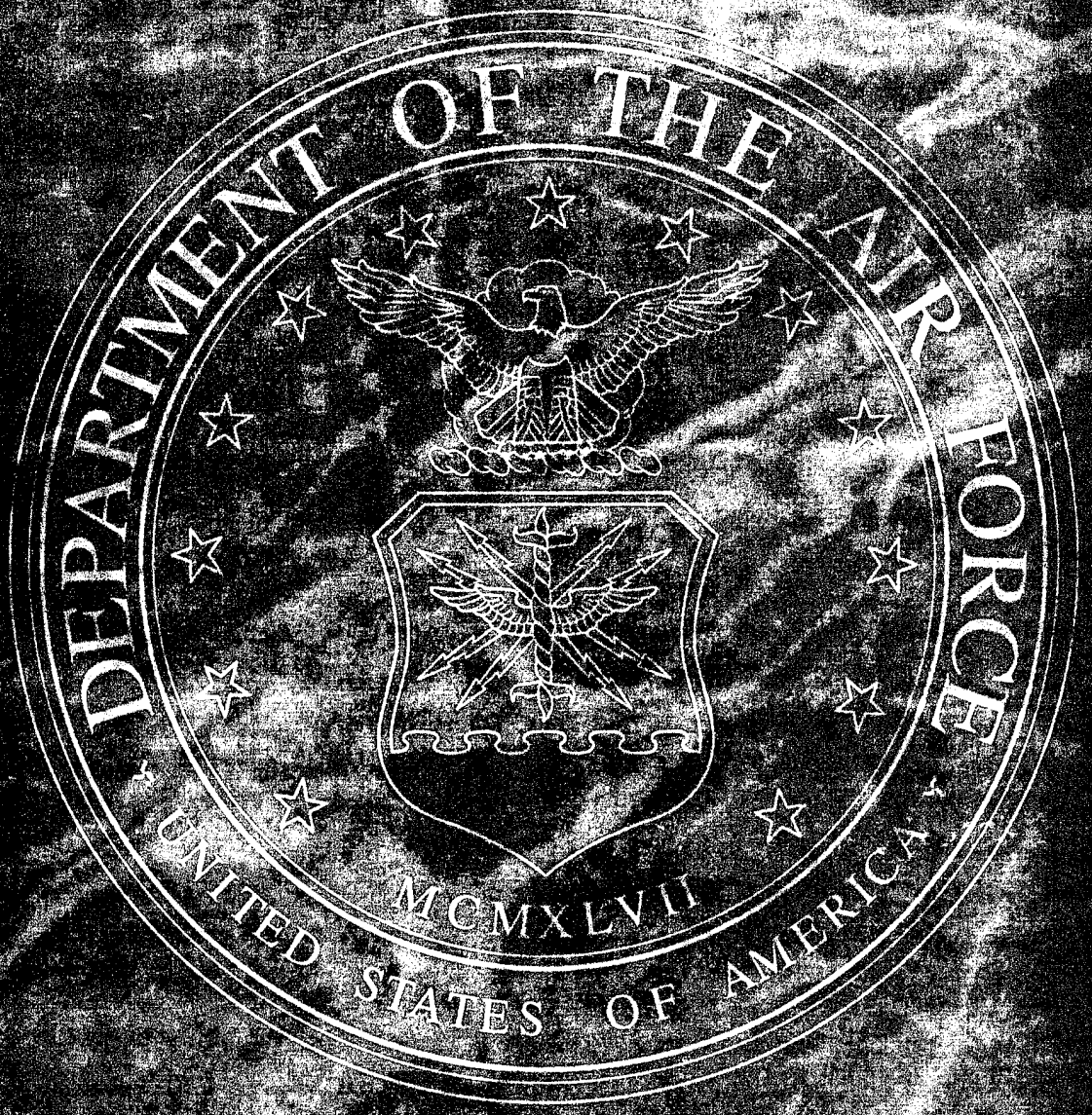
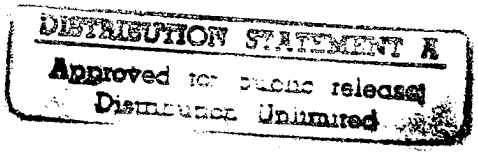


CORNERSTONES
OF INFORMATION WARFARE

Approved for public release
Distribution Unlimited

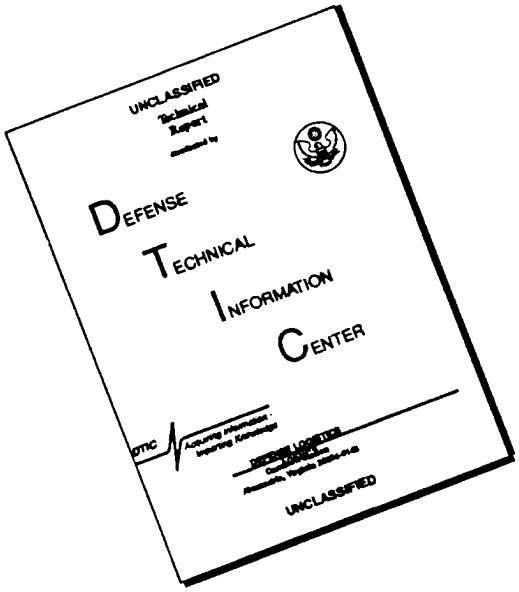
CORNERSTONES
OF INFORMATION WARFARE



19960501 159

DTIC QUALITY INSPECTED 1

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

FOREWORD

As information systems permeate our military and civilian lives, we are crossing a new frontier – the Information Age. It will define the 21st century and influence all we do as an air force. Information Warfare has become central to the way nations fight wars, and will be critical to Air Force operations in the 21st century. This means, of course, that today we must invest in our people, planning, equipment, and research so our ambitions can become reality. We will involve every Air Force person in this effort, generating a wave of momentum that will carry us into the next millennium.

Information Warfare is not the exclusive domain of the Air Force, or any other service. Information technology advances will make dramatic changes in how this nation fights wars in the future. They will allow a commander's vision and view of the battlespace to be shared at the lowest level. Because of this, every practitioner of the profession of arms has a responsibility to understand the impact of information warfare on their service. From our unique perspectives as soldier, sailor, marine, or airman, we can then forge a common understanding of how to use information warfare to enhance joint warfighting capabilities.

Ronald R. Fogleman
General, USAF
Chief of Staff

Sheila E. Widnall
Secretary of the Air Force

CORNERSTONES OF INFORMATION WARFARE

The competition for information is as old as human conflict. It is virtually a defining characteristic of humanity. Nations, corporations, and individuals each seek to increase and protect their own store of information while trying to limit and penetrate the adversary's. Since around 1970, there have been extraordinary improvements in the technical means of collecting, storing, analyzing, and transmitting information. Reams have been written about the impact of this technical revolution on the conduct of war, particularly since DESERT STORM. However, most of the literature focuses primarily on technical developments, not on how these developments impact doctrine.

This paper will pose questions important to Air Force policy makers and provide answers firmly grounded on concise definitions, institutional experience, and doctrinal concepts. In the process, it will clarify why the competition for information, which predates the dawn of history, is suddenly a riveting national security topic. Closer to home, this paper will also describe how Air Force doctrine should evolve to accommodate information warfare. The ultimate goal is a sound foundation on which to base the inevitable changes in organizing, training, equipping, and employing military forces and capabilities.

WHY ARE WE TALKING ABOUT INFORMATION NOW?

Because there is a technological revolution[1] sweeping through information systems and their integration into our daily lives leading to the term "Information Age." Information-related technologies concentrate data, vastly increase the rate at which we process and transmit data, and intimately couple the results into virtually every aspect of our lives. The Information Age is also transforming **all** military operations by providing commanders with information unprecedented in quantity and quality.[2] The commander with the advantage in observing the battlespace, analyzing events, and distributing information possesses a powerful, if not decisive, lever over the adversary.

1. The technological basis of information systems has radically changed since roughly 1970. These changes include increases in storage density, access speed, instruction rates, and communication rates, plus decreases in size and weight. Because of these changes, information systems now permeate our lives. We consider this *prima facie* evidence of a revolution. However, this paper does not intend to answer the question of whether these changes constitute a revolution, or merely an evolution.

2. Quality here refers to concepts such as timeliness, specificity, and accuracy.

Before continuing, we must distinguish between *information age warfare* and *information warfare.* We make this distinction because much of the literature treats information warfare and advances in information technology synonymously. Information age warfare uses information technology as a tool to impart our combat operations with unprecedented economies of time and force.[1] Ultimately, information age warfare will affect *all* combat operations. **In contrast, information warfare, the point of this paper, views information itself as a separate realm, potent weapon, and lucrative target.** Information, as we will show below, is technology independent. However, information age technology is turning a theoretical possibility into fact: *directly*[2] manipulating the adversary's information. This is the driving force behind this paper.

WHAT IS INFORMATION?

This question is elementary, but pivotal. It is impossible to discuss information warfare meaningfully without rigorously defining the central concept: information.

Information derives from phenomena. Phenomena, observable facts or events, are *everything* that happens around us. Phenomena must be perceived and interpreted to become information. Information, then, is the result of two things: perceived phenomena (data) and the instructions required to interpret that data and give it meaning.

This distinction is important, and easily encompassed by a familiar paradox: If a tree falls, but no one was around to hear it, did it make a noise? The falling tree caused pressure waves in the atmosphere, a phenomenon. Noise, the information denoting a falling tree, occurs when someone's ear detects the pressure waves, creating data, and the brain's instructions manipulate that data into the sound recognizable as a falling tree. Within that person's context, there is no falling tree until the person hears (or sees) it.

Phenomena become information through observation and analysis. Therefore, information is an abstraction of phenomena. Information is the result of our perceptions and interpretations, regardless of the means. As falling trees make clear, to define information requires only two characteristics:

Information: *data and instructions.*

Note that the definition for information is absolutely distinct from technology. However, what we can do with information, and how fast we can do it, is *very* dependent on technology. Technology dramatically enhances our observational means, expands and concentrates data storage, and accelerates instruction processing. We use the following term to encompass the technology-dependent elements associated with information:

1. Cruise missiles exploit information age technologies to put a bomb on target. This is an example of information age warfare – using information age technologies as tools to better perform combat operations.

2. Direct manipulation changes the adversary's information *while completely bypassing the adversary's perceptive, analytical, or decision processes.*

Information Function: *any activity involving the acquisition, transmission, storage, or transformation of information.*

For example, the system that tells a machine to stamp eighty hubcaps is performing an information function. The sheet metal press stamping those hubcaps is not.

WHAT ARE SOME MILITARY INFORMATION FUNCTIONS?

Quality information is the counter to the fog of war. As mentioned earlier, the commander with better information holds a powerful advantage over his adversary. Military operations make special demands on information functions in seeking to give the commander an information advantage.

Surveillance and reconnaissance are our powers of observation. Intelligence and weather analysis are the bases for orienting observations. We use those bases to form an Air Tasking Order, which command and control operations execute and monitor in directing the conflict. Precision navigation enhances mission performance. Together, these are the kinds of military information functions that enhance *all* military operations. Collectively, we use the term military information functions to describe force enhancing information functions.

Military Information Function: *any information function supporting and enhancing the employment of military forces.*

This definition serves to delineate militarily important information functions from the total universe of information functions.

WHAT IS INFORMATION WARFARE?

At the grand strategy level, nations seek to acquire, exploit, and protect information in support of their objectives. This exploitation and protection can occur in the economic, political, or military arenas. Knowledge of the adversary's information is a means to enhance our own capabilities, degrade or counteract enemy capabilities, and protect our own assets, *including our own information.* This is not new. The struggle to discover and exploit information started the first time one group of people tried to gain advantage over another.

Information warfare consists of targeting the enemy's information and information functions, while protecting our own, with the intent of degrading his will or capability to fight.[1] Drawing on the definitions of information and information functions, we define information warfare as:

Information Warfare: *any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting*

1. There is a troubling offense–defense asymmetry in the scope of information warfare. The military may, consistent with the law of armed conflict, attack any militarily significant target. In the context of information warfare, this means we may target any of the adversary's information functions that have a bearing on his will or capability to fight. In stark contrast, our military may defend only military information functions. There are many information functions critical to our national security that lie outside the military's defensive purview.

ourselves against those actions; and exploiting our own military information functions.[1]

This definition is the basis for the following assertions:

Information warfare is any attack against an information function, regardless of the means. *Bombing a telephone switching facility is information warfare. So is destroying the switching facility's software.*

Information warfare is any action to protect our information functions, regardless of the means. *Hardening and defending the switching facility against air attack is information warfare. So is using an anti-virus program to protect the facility's software.*

Information warfare is a means, not an end, in precisely the same manner that air warfare is a means, not an end. *We may use information warfare as a means to conduct strategic attack and interdiction, for example, just as we may use air warfare to conduct strategic attack and interdiction.*

Militaries have always tried to gain or affect the information required for an adversary to effectively employ forces. Past strategies typically relied on measures such as feints and deception to influence decisions by affecting the decision maker's perceptions. Because these strategies influenced information through the perception process, they attacked the enemy's information *indirectly.* That is, for deception to be effective, the enemy had to do three things:

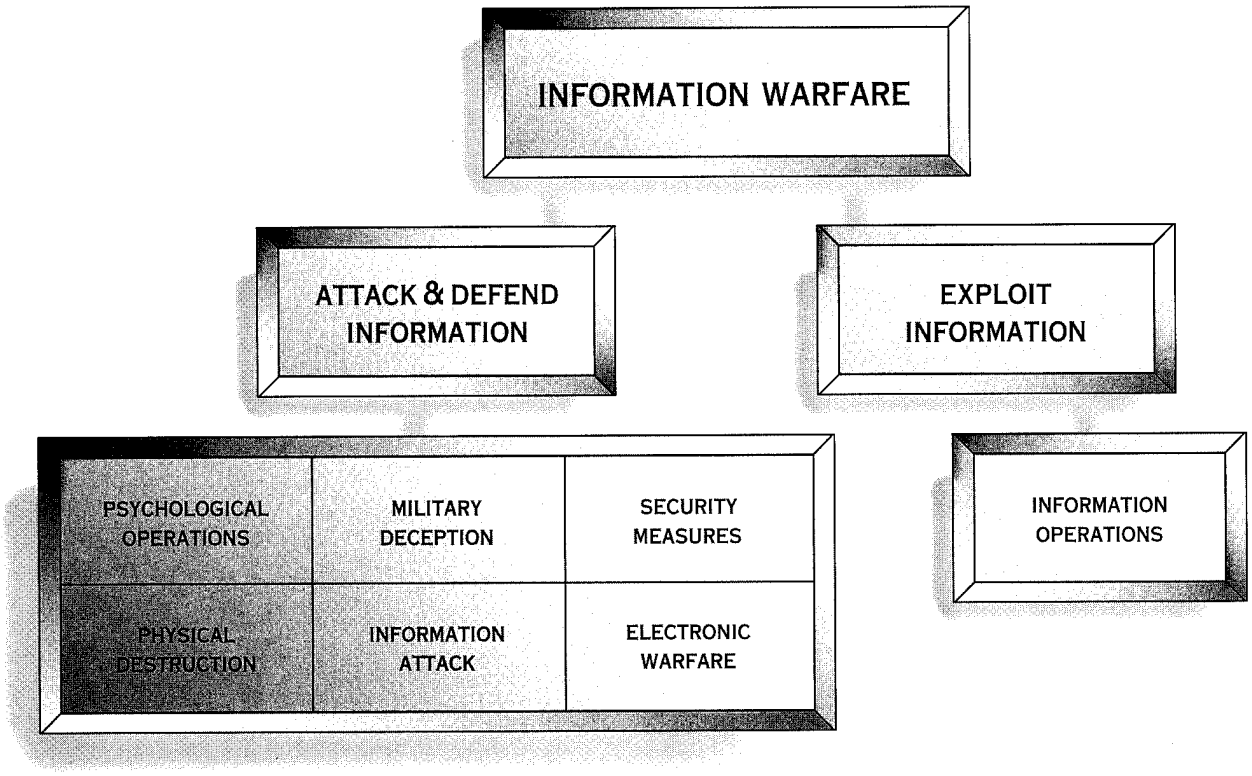
- observe the deception,
- analyze the deception as reality, and
- act upon the deception according to the deceiver's goals.

However, modern means of performing information functions give information added vulnerability: *direct* access and manipulation.[2] Modern technology now permits an adversary to change or create information without relying on observation and interpretation. Here is a short list of modern information system characteristics creating this vulnerability: concentrated storage, access speed, widespread information transmission, and the increased capacity for information systems to direct actions autonomously. Intelligent security measures can reduce, but not eliminate, this vulnerability; their absence makes it glaring.

Militaries are not inclined to trust their success to the fortunes of war. So we must direct our information warfare efforts to more than just targeting an adversary's information: we must also defend our own information, and all its operations. The Air Force depends heavily upon military information functions, making us vulnerable to information warfare. The integrity of our military information functions, as well as the information itself,

1. Note, this definition depends only on the nature of the action, not how it is accomplished.

2. To reiterate: **Indirect Information Warfare:** changing the adversary's information by creating phenomena that the adversary must then observe and analyze. Electronic warfare, when used to degrade the adversary's ability to accurately perceive phenomena, is conducting indirect information warfare. **Direct Information Warfare:** changing the adversary's information without involving the intervening perceptive and analytical functions. Replacing bar code labels with bogus ones on pallets in a deployment staging area is a form of direct information warfare.



bears heavily and directly on the success of our military operations.

WHAT COMPRISES INFORMATION WARFARE?

Recalling the definition, information warfare consists of activities that deny, exploit, corrupt, destroy, or protect information. Traditional means of conducting information warfare include psychological operations, electronic warfare, military deception, physical attack, and various security measures.

Psychological Operations *use information to affect the enemy's reasoning.*

Electronic Warfare *denies accurate information to the enemy.*[1]

Military Deception *misleads the enemy about our capabilities or intentions.*[2]

Physical Destruction *can do information warfare by affecting information system elements through the conversion of stored energy to destructive power. The means of physical attack range from conventional bombs to electromagnetic pulse weapons.*

Security Measures *seek to keep the adversary from learning about our military capabilities and intentions.*[3]

1. Note, this paper uses the JCS recognized label "electronic warfare" instead of "electronic combat."

2. Military deception provides an excellent example of how actions are defined by their ends, not means. Air power may conduct information warfare through military deception, as in World War II's Operation FORTITUDE NORTH, where the Allies dropped two bombs in the Pas de Calais for each bomb dropped in Normandy, a successful effort to mislead the Germans about our invasion plans.

3. Current security measures include OPSEC, COMSEC, and COMPUSEC. As information technology changes, these security measures will almost certainly evolve into entirely different forms.

The Information Age has provided new and practical means to deny, exploit, corrupt, or destroy information,[1] as well as the vulnerabilities to make those attacks possible. Air Force doctrine does not yet acknowledge or define these assaults on information, which we call Information Attack.

Information Attack: *directly corrupting*[2] *information without visibly changing the physical entity within which it resides.*

Information attack, constrained by the definition of information, is limited to directly altering data or instructions. It is, therefore, just another means of conducting information warfare, one whose immediate effects do not include visible changes to the entity within which the information resides. That is to say, after being subjected to information attack, an information function is indistinguishable from its original state except through inspecting its data or instructions.[3]

How Is Information Attack Different?

As previously described, there are two ways to influence the adversary's information functions: indirectly and directly.

Indirect information warfare affects information by creating phenomena, which the adversary will perceive, interpret, and act upon. Military deception, physical attack, and OPSEC traditionally achieved their ends indirectly.[4] For example, the goal of deception is to cause the adversary to make incorrect decisions; deception does this by creating an apparent reality. Generally, this entails creating phenomena for the enemy to observe. Success, however, depends on several conditional events: the adversary actually observes the phenomenon, thereby turning it into data; analyzes it into the desired information; and acts upon the information in the desired manner.

Direct information warfare affects information through altering its components without relying on the adversary's powers of perception or interpretation. Information attack acts directly upon the adversary's information. Since nearly all modern information functions are themselves controlled by information, information attack may be directed against most information functions.

Direct information warfare, the point of information attack, acts on the adversary's information without relying on the

1. Examples: Cutting the radar to command center landline is information denial. Insider trading is information exploitation. Altering a barcode is information corruption. Reformatting someone's hard drive is information destruction.

2. Corruption covers the spectrum from subtle alteration to thorough destruction.

3. A SOF team dropping a powerful magnet on a hard disk is an example of information attack.

4. Military deception creates an alternate reality upon which the adversary will base his decisions; psychological operations target the will to fight; physical attack creates phenomena for the adversary to perceive and convert into information; OPSEC denies the enemy knowledge of our own operations.

adversary's collection, analysis, or decision functions. It can short circuit the OODA loop[1] through creating observations and skewing orientation, or decapitate it by imposing decisions and causing actions.

A short illustration will serve to demonstrate the difference between indirect and direct information warfare applications:

Our goal, using military deception, is to make the adversary think there is a wing of combat aircraft where, in fact, there is none, and act on that information in a manner benefitting our operations.

Indirect information warfare: Using military deception, we could construct fake runways and parking areas, and generate enough other activities to present a convincing image. We rely on the adversary to observe the pseudo combat operation and interpret it as real (as opposed to detecting the fake). Only then does it become the information we want the adversary to have.

Direct information warfare: Conversely, if we use information attack to create the pseudo combat wing in the adversary's store of information, the result–deception–is precisely the same. But the means to that result, never mind the resources, time, and uncertainty, are dramatically different.

What Is The Other Edge Of The Information Warfare Sword?

The defensive side of information warfare–security measures aimed at protecting information–prevents an adversary from conducting successful information warfare against our information functions. Current security measures such as OPSEC and COMSEC are typical means of preventing, detecting, and subverting an adversary's *indirect* actions on our military information functions. In contrast, security measures such as COMPUSEC encompass preventing, detecting, and subverting *direct* information actions on our information functions. Future security measures must evolve as information technology advances. Consequently, new measures will likely take forms entirely different from today's security measures, rooted as they are in previous security requirements. As the simple examples in this paper illustrate, we must avoid falling victim to profound, debilitating effects of direct information warfare.

Why Is Information Warfare Important To The USAF?

Two reasons. First, because information warfare offers important means to accomplish Air Force missions. Second, because the widespread integration of information systems into Air Force operations makes our military information functions a valuable target set.

1. OODA Loop: Observe, Orient, Decide, and Act. Observation converts phenomena into data. Orientation processes the data into information. Decide converts the information into orders. Act converts the orders into action. The OODA loop is continuous—as you act you observe the results, starting the process all over again.

A hypothetical example using information attack shows how information warfare might accomplish a typical Air Force mission:

Interdiction prevents or delays essential resources from reaching combat units. One approach to interdiction is wrecking bridge spans using laser-guided bombs. Alternatively, we might be able to alter the adversary planners' information, falsely categorizing the bridges as destroyed, causing the planners to reroute forces and supplies. Each means performs interdiction; information attack offers the possibility of achieving our goal while consuming fewer resources or without exposing our assets to attack.

As an example emphasizing the need for robust defenses against information warfare, imagine the chaos that would ensue should an adversary manage to penetrate our time-phased force deployment database. Subtle changes in it could be sufficient to bring our power projection capabilities to a near standstill.

How Should We Change Air Force Doctrine To Accommodate Information Warfare?

Presently, Air Force doctrine recognizes air warfare and space warfare. However, the doctrine doesn't identify separate missions for air warfare or space warfare. Instead, both cut across all roles and missions. Similarly, information warfare cannot be pigeonholed as a single mission. To do so would fail to completely integrate information warfare into Air Force doctrine.

Recall that missions are operational tasks performed to achieve military objectives. Air warfare is a means, defined by the environment, to execute those missions. There are three objectives of air warfare:

- **control** the air while protecting our forces from enemy action,
- **exploit** control of the air to employ forces against the enemy, and,
- **enhance** our overall force effectiveness.

In our doctrine, the *objectives* of control, exploit, and enhance translate into the *roles* of aerospace control, force application, and force enhancement.

In many respects, one can consider information as a realm, just as land, sea, air, and space are realms.[1] Information has its own characteristics of motion, mass, and topography, just as air, space, sea, and land have their own distinct characteristics.[2] There are strong conceptual parallels between conceiving of air and information as realms. Before the Wright brothers, air, while it obviously existed, was not a realm suitable for practical, widespread military operations. Similarly, information existed before the

1. **realm**, *n*: the region, sphere, or domain within which anything occurs, prevails, or dominates. [The Random House College Dictionary]

2. Land, sea, air, and space are realms within which we may conduct military operations. Each realm imposes its characteristics on operations within it. Information and its functions also may host military operations, but those operations must conform to the characteristics of the information system and its functions.

Information Age. But the Information Age changed the information realm's characteristics so that widespread military operations within it became practical.

Information warfare, like air warfare, is the means defined by the environment to execute military missions. There are three objectives of information warfare:

- **control** the information realm so we can exploit it while protecting our own military information functions from enemy action,
- **exploit** control of information to employ information warfare against the enemy, and,
- **enhance** overall force effectiveness by fully developing military information functions.

The **first** objective of information warfare, to **control** the realm so we can exploit it while protecting our own military information functions from enemy action, contributes significantly to controlling the combat environment. Presently, Air Force doctrine recognizes two missions to control the combat environment: counterair and counterspace. Counterair comprises missions whose objectives are control of the air; counterspace comprises those missions whose objectives are control of space. Clarity and consistency require we term those activities dedicated to controlling information as *counter-information.*

Counterinformation: *actions dedicated to controlling the information realm.*

Further, counterinformation, like counterair and counterspace, has both offensive and defensive aspects. Offensive counter-information enables us to use the information realm and impedes the adversary's use of the realm. Typical means include physical attack, military deception, psychological operations, electronic warfare, and information attack. Defensive counterinformation includes both active and passive actions to protect ourselves from the adversary's information warfare actions. Defensive counterinformation is accomplished, for instance, through physical defense, physical security, hardening, OPSEC, COMSEC, COMPUSEC, and counterintelligence.

Successful aerospace control enables us to use the air and space realms without suffering substantial losses, and inflict substantial losses on the enemy's use of those realms. Counterinformation, working with counterair and counterspace, seeks to create such an environment.

The **second** objective of information warfare is to **exploit** our control of information. In air warfare's force application role, the missions of strategic attack, interdiction, and close air support exploit air control. Similarly, information warfare might also be used to achieve the same ends. We have already cited an example of how information warfare can perform interdiction. It can also perform strategic attack:

Suppose we want to limit the enemy's long-term mobility by restricting his POL resupply. We first identify his refineries as the most suitable target to achieve this goal. Through research we further identify the specific refineries comprising most of his production capacity. For each refinery, we find there is one critical cracking tower. We mount a strike and, with admirable economy of force, put the refineries out of operation by destroying just those towers, while leaving everything else untouched. This is a classic example of strategic attack.

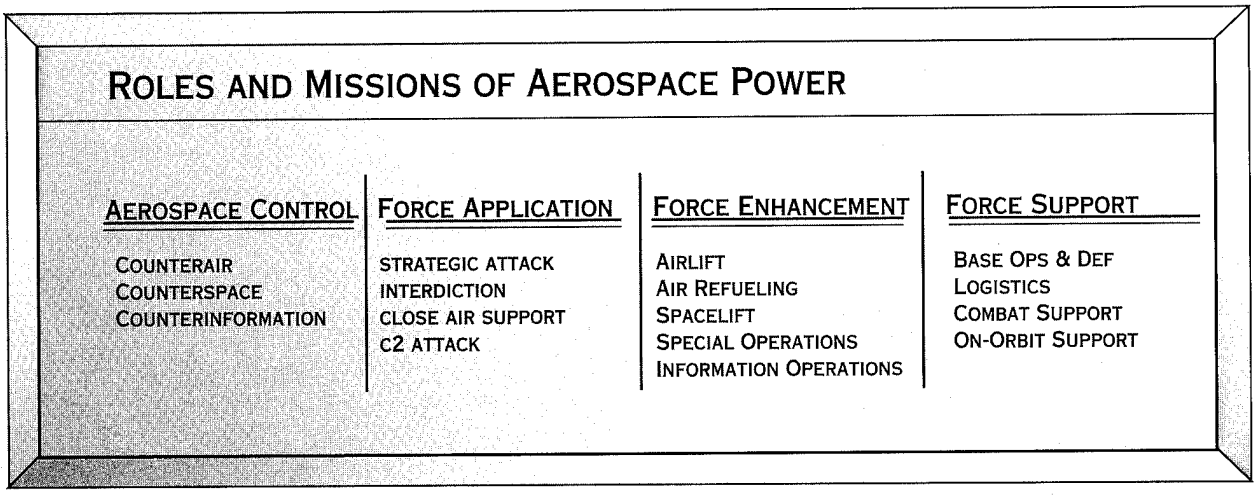
Same situation. Like all modern refineries, these have extensive automated control systems. These extensive information functions offer a potential target for information warfare. Early in the conflict we performed an offensive counterinformation mission by penetrating and characterizing the refinery's automated control system. In the process, we uncovered several vulnerable information dependencies, giving us the means of affecting the refineries' operations at a time of our choosing. Later in the conflict, combined with interdiction and ground maneuvers, we choose to exploit one of the vulnerabilities. We have just disabled their refineries. This, too, is a classic example of strategic attack.

Information technology is already tightly woven with our military operations, providing heretofore unimaginable amounts of information. Exploiting this information has provided us striking capabilities; relying on it inevitably creates potentially crippling vulnerabilities. This, coupled with advances in the ability to both locate and destroy command and control (C2) nodes makes C2, more than ever, a lucrative target set. History has shown successful militaries can achieve striking success through paralyzing the enemy's ability to exercise command and control. Airmen have always considered this an important objective and expended much effort against C2.[1] For these reasons, the efforts to disrupt and destroy the adversary's command and control elements have prompted us to identify a separate mission under force application.

C2 Attack: *any action against any element of the enemy's command and control system.*

The **third** objective of information warfare is to develop information functions to **enhance** total force effectiveness. Previously we described military information functions as supporting the employment of military forces. Our current doctrine does not include such a mission. To fill that void, we will include information operations under force enhancement. Some examples of information operations are: surveillance, reconnaissance, command and control, communications, combat identification, intelligence, precision navigation, and weather. The distinguishing characteristic of the information operations mission is that it deals primarily with information as both its resource and product.

1. Consider, for example, DESERT STORM, or Israel's domination of the air over the Bekaa Valley in 1982. Reaching further into the historical record, in the initial stages of General Allenby's 1918 Palestine Campaign, Allied aircraft attacked key Turkish telephone exchanges, destroying communications among Turkish forces. Consequently, the Fourth Army remained in bivouac for four days, unaware of the disaster befalling other Turkish forces to their west.



Information Operations: *any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces.*

Since we require relevant, accurate, and timely information for *everything* we do, information operations support the conduct of missions across all four roles, from aerospace control to force support. Information operations provide commanders the ability to observe the battlespace, analyze events, and direct forces. Information operations provide logisticians the ability to know what is in inventory, and where it is needed. Information operations provide the flight lead the ability to know where the target is, its defenses, and select the most appropriate weapon.

In sum, information warfare cuts across all Air Force roles and missions. It is another means to conduct our traditional missions. However, there are three additional operational tasks that information warfare enables us to execute which are not suitably addressed by our current doctrine: counterinformation, C2 Attack, and information operations. Similarly, we elected to delete two missions no longer relevant under regrouped missions: electronic combat, previously under force enhancement, is now subsumed by information warfare; surveillance and reconnaissance are now considered instances of information operations. However, this list is by no means exhaustive. As this paper's title conveys, the ideas contained herein provide the cornerstones, not the entire building. Invariably, as the Air Force fully accommodates the information technology revolution, additional operational tasks may arise which will in turn warrant adding or removing missions. To the extent these cornerstones continue to provide a valid litmus test for information warfare, all new missions need to meet and pass it.

What Is The Relationship Between Information Warfare And Command & Control Warfare?

The focus of information warfare is *any* information function, whether it is C2, a refinery's control system, or a telephone switching station. C2 represents only part of the universe of military information functions. The Joint Staff defines command and control:

Command and Control: *the exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. [Joint Pub 1-02]*

Command and control warfare (C2W) only addresses activities directed against the adversary's ability to direct the disposition and employment of forces, or those which protect the friendly commander's ability to do so. As we have illustrated, information warfare not only attacks the C2 process, but it also attacks the enemy's combat power itself. Conversely, by definition, C2W is not associated with reducing or nullifying the ability or desire of combat units to execute their orders. Tactical psychological operations and electronic countermeasures self-protection hinder the ability of units to execute orders. But they in no way affect commanders' ability to issue orders to those units, nor their ability to receive those orders.

Although extraordinarily important, the JCS's policy of Command and Control Warfare is only a particular application of information warfare. For the military to concentrate only on C2W would be ignoring other legitimate target sets. Therefore, information warfare, and its attendant organizing, training, and equipping issues, is essential to fully effective C2W.

Is Information Warfare Important Only To The Air Force?

We have established that information warfare is important to the Air Force for two reasons. First, since our military information functions present a valuable target set, we must make commensurate defensive efforts. Second, as the examples in this paper show, information warfare is a potential means to achieve typical Air Force ends: strategic attack, interdiction, etc. More fundamentally, the Air Force *already does* information warfare through such systems as the EF-111 and Compass Call.

But in a broader sense, information warfare might be a means to conduct any mission the services already conduct – and the services are best positioned to choose the best means for their ends. Each service has its own unique operational demands. After all, the Army is best qualified to decide

which means are best suited for pursuing the goals the Joint Force Commander apportions to the Army.

As a result of its service-unique expertise, its own OODA loop requirements, logistics, etc., each service has information warfare concerns. In developing the doctrinal constructs in this paper, we used airpower terminology and examples. That is our background, those are the terms and the environment with which we are familiar. But the argument we present **is not** dependent on terminology. Replacing Air Force terms with Army or Navy terms would leave the conclusions unchanged.

CONCLUSION

The information revolution, startlingly fast as it is, shows no signs of slowing. As the Air Force becomes more technologically sophisticated, it becomes more technologically dependent. We need to use that technological sophistication to avail ourselves of all the opportunities that information, as a target, presents. We also need to be aware that our technical dependencies represent potentially crippling vulnerabilities. Sophisticated, robust, multi-layered defenses for our military information functions may well be what separates us from joining the sorry league of military failures.

Information, combined with modern information functions, has distinct characteristics that warrant it being considered a realm, just as land, sea, air, and space are realms. Information warfare does not fill a discrete place in Air Force doctrine. Just like air warfare, information warfare can be part of many AFM 1-1 missions. Just as when space warfare was integrated into Air Force doctrine, viewing information as a realm now leads us to add several missions:

Counterinformation: *controlling the information realm.*

C2 Attack: *any action against the enemy's command and control system.*

Information Operations: *any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces.*

Since World War I, airmen have had to control the air environment effectively to employ airpower. What is more, air and space superiority are virtually a *sine qua non* for employing ground and naval forces. Information is the next realm we must control to operate effectively and with the greatest economy of force.

At the outset we stated the competition for information is as old as man's first conflict. It involves increasing and protecting our own store of information while limiting and penetrating the adversary's. The recent explosion in information technologies is prompting the current discussion in and outside government on the topic of information warfare – targeting the enemy's information functions, while protecting ours, with the intent of degrading his will or capability to fight.

For airmen, controlling the combat environment is Job One. With the advances in information technology, airmen must pursue information superiority just as they do air and space superiority. Only with these realms under our control can we effectively employ **all** our combat assets. Military information functions are essential to our combat operations–they are a tool for achieving the Joint Force Commander's campaign objectives. Targeting the enemy's information functions keeps him from achieving his.

In this paper we have laid out information warfare's doctrinal foundation. Our goal is to provide a sound and widely accepted basis from which we can adapt Air Force doctrine to the Information Age. The ultimate aim? Incorporating information warfare into the way the Air Force organizes, trains, equips, and employs.

DEFINITIONS

C2 Attack: Any action against any element of the enemy's command and control system.

Command and Control: The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission.

Counterinformation: Actions dedicated to controlling the information realm.

Defensive counterinformation: Actions protecting our military information functions from the adversary.

Direct Information Warfare: Changing the adversary's information without involving the intervening perceptive and analytical functions.

Indirect Information Warfare: Changing the adversary's information by creating phenomena that the adversary must then observe and analyze.

Information: Data and instructions.

Information Attack: Directly corrupting information without visibly changing the physical entity within which it resides.

Information Function: Any activity involving the acquisition, transmission, storage, or transformation of information.

Information Operations: Any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces.

Information Warfare: Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.

Military Information Function: Any information function supporting and enhancing the employment of military forces.

Offensive counterinformation: Actions against the adversary's information functions.